Framework External Authentication Reference Manual

Kerberos External Authentication

12/13/2025

Kerberos External Authentication

Contents

Configuration Server and Configuration Server Proxy support the use of the Kerberos authentication protocol for user authentication in Genesys user interface applications. Kerberos enables secure communication between nodes over a non-secure network, using tickets to enable the nodes to prove their identity to each other in a secure manner.

Configuration Server uses Windows Active Directory and MIT key distribution centers to implement Kerberos authentication.

Kerberos vs RADIUS/LDAP

Kerberos, RADIUS, and LDAP are all types of external authentication. However, Kerberos differs slightly from the existing external authentication protocols (RADIUS, LDAP, and others) in when the authentication is performed, as follows:

Existing external authentication protocols operate in “in behind” mode. That is, the authentication is carried out when the interface application sends the request to Configuration Server, which then forwards it to the authentication system.

Kerberos operates in “in front” mode. The authentication is activated on the client side before a connection to Configuration Server is made. When the actual connection to Configuration Server is made, the interface gets an authentication ticket (a Kerberos token) that is already authenticated. This ticket is sent to Configuration Server with the login request to assert that authentication is already done.

Supported Environments

Configuration Server supports Kerberos authentication on the following platforms:

- Red Hat Enterprise Linux (RHEL) version 5 and later
- Windows 2008 and later
- Solaris version 10 and later
- AIX version 5.3 and later

The following versions of MIT Kerberos are used:

- krb5-1.11 for supported UNIX platforms
- kfw-4.0.1 for Windows